UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/755,660	01/05/2001	Roy Franklin Quick JR.	PA010055	4954

23696 7590 08/10/2004

Qualcomm Incorporated
Patents Department
5775 Morehouse Drive
San Diego, CA 92121-1714

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	11

DATE MAILED: 08/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/755,660	QUICK ET AL.	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending the application.

2. Claims 1-21 stand being rejected.

Response to Amendment

3. The examiner approves the new title.

Response to Arguments

4. Applicant's arguments filed 5/24/04 have been fully considered but they are not persuasive.

On page 4, the applicant argues that Rogaway does not disclose or even suggest generating a plurality of keys in response to a received challenge as in independent claim 1.

The examiner respectfully disagrees. There is a challenge for authentication between communication partners A and B. From this challenge a long-lived key and a shared key is generated. That is two keys being generated, therefore constitutes a plurality of keys.

On page 4, the applicant argues that Reeds does not discloses or even suggest a subscriber identification module comprising a key generation element and a signature generator configured to receive a secret key from the key generation element as in independent claim 6. The applicant argues that Reeds does not disclose a key generator for generating a plurality of keys and a signature generator as in independent claim 10. The applicant argues that Reeds does not discloses generating a plurality of keys and transmitting at least one key from the plurality of keys to a communication device communicatively coupled to a subscriber identification device as in independent claims 16 and 21.

The examiner respectfully disagrees. Reeds does not explicitly discloses a key generation element. However, the mobile units contain a secret A-key. The key would not exist

if there were no key generation element. Reeds discloses signature generation during the jumble process. Reeds discloses the secret A-key as well as a public key. That is two keys being generated, therefore constitutes a plurality of keys.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 2, 4 and 5 are rejected under 35 U.S.C. 102(b) as being anticipated by Rogaway U.S. Patent No. 5,491,749.

As to claim 1, Rogaway discloses a memory and a processor configured to implement a set of instructions stored in the memory [column 10, lines 24-42]. Rogaway discloses generating a plurality of keys in response to a received challenge [column 7 line 39 to column 8 line 55]. Rogaway discloses generating an authentication signal based on a received signal and a first key from the plurality of keys [column 8, lines 33-47]. Rogaway discloses that the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module [column 8, lines 33-47]. Rogaway discloses that the received signal is generated by the communications unit using a second key from the plurality of keys [column 8, lines 48-67]. Rogaway discloses that the second key has been communicated from the subscriber identification module to the communications unit [column 9 line 26 to column 10 line 54]. Rogaway discloses transmitting the authentication signal to the communications system via the communications unit [column 9 line 26 to column 10 line 54].

As to claim 2, Rogaway discloses that the authentication signal is generated by a hash function [column 9, lines 1-22].

As to claim 4, Rogaway discloses that the authentication signal is generated by an encryption algorithm [column 9, lines 35-62].

As to claim 5, Rogaway discloses that the encryption algorithm is the Data Encryption Standard (DES) [column 9, lines 35-62].

6. Claims 6-14, 16-19 and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Reeds, III U.S. Patent No. 5,204,902.

As to claim 6, Reeds discloses a key generation element [column 4, lines 32-46]. Reeds discloses a signature generator configured to receive a secret key from the key generation element and information from a mobile unit, and further configured to output a signature to the mobile unit [column 5, lines 25-33].

As to claim 7, Reeds discloses a memory and a processor configured to execute a set of instructions stored in the memory [column 4, lines 27-31]. Reeds discloses that the set of instructions performs a cryptographic transformation upon an input value to produce a plurality of temporary keys [column 4, lines 27-31].

As to claim 8, Reeds discloses that the cryptographic transformation is performed using a permanent key [column 6, lines 3-23].

As to claim 9, Reeds discloses a memory and a processor configured to execute a set of instructions stored in the memory, as discussed above. Reeds discloses that the set of instructions performs a cryptographic transformation upon the information from the mobile unit

by using the secret key [column 6, lines 3-23]. Reeds discloses that the signature results from the cryptographic transformation [column 5, lines 25-33].

As to claim 10, Reeds discloses a key generator for generating a plurality of keys from a received value and a secret value [column 4, lines 32-46]. Reeds discloses that at least one communication key from the plurality of keys is delivered to the communications unit and at least one secret key from the plurality of keys is not delivered to the communications unit [column 4, lines 32-46]. Reeds discloses a signature generator for generating an authorization signal from both the at least one secret key and from an authorization message, as discussed above. Reeds discloses that the authorization message is generated by the communications unit using the at least one communication key [column 6, lines 36-60].

As to claim 11, Reeds discloses that the subscriber identification module is configured to be inserted into the communications unit [column 4, lines 27-31].

As to claim 12, Reeds discloses that the signature generator generates the authorization signal by using a hash function [column 6, lines 36-60].

As to claim 13, Reeds discloses that the signature generator generates the authorization signal by using the Data Encryption Standard (DES) [column 9, lines 28-44].

As to claim 14, Reeds discloses that at least one communication key comprises an integrity key [column 10, lines 18-24].

As to claim 16, Reeds discloses generating a plurality of keys, as discussed above. Reeds discloses transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys, as discussed above. Reeds discloses generating a signature at the

communications device using both the at least one key transmitted to the communications device and a transmission message, as discussed above. Reeds discloses transmitting the signature to the subscriber identification device [column 9, lines 1-25]. Reeds discloses receiving the signature at the subscriber identification device [column 9, lines 47-63]. Reeds discloses generating a primary signature from the received signature [column 9, lines 47-63]. Reeds discloses conveying the primary signature to a communications system [column 9, lines 47-63].

As to claim 17, Reeds discloses that the generating of the signature signal is performed using a nonreversible operation. As discussed above the signature is created with a hash. The examiner asserts that a hash is a nonreversible operation.

As to claim 18, Reeds discloses that the generating of the signature signal is performed using DES, as discussed above.

As to claim 19, Reeds discloses that the generating of the signature signal is performed using a hash function, as discussed above.

As to claim 21, Reeds discloses generating a plurality of keys, as discussed above. Reeds discloses transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys, as discussed above. Reeds discloses assigning a weight to the transmission message at the communications device in accordance with a relative importance of the transmission message [column 9, lines 28-44]. Reeds discloses generating a signature at the communications device using both the at least one key transmitted to the communications device and the transmission message, as discussed above. Reeds discloses transmitting the signature to a communications system if the assigned weight to the transmission message indicates that the

transmission message is unimportant [column 10, lines 12-37]. Reeds discloses transmitting the signature to the subscriber identification device if the assigned weight to the transmission message indicates that the transmission message is important [column 10, lines 12-37]. Reeds discloses that the subscriber identification device generates a primary signature from the received signature signal, as discussed above. Reeds discloses conveying the primary signature to a communications system, as discussed above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rogaway U.S. Patent No. 5,491,749 as applied to claim 1 above, and further in view of Applied Cryptography (hereinafter Schneier).

As to claim 3, Rogaway discloses using hash functions, as discussed above.

Rogaway does not teach that the hash function is the Secure Hash Algorithm (SHA-1).

Schneier teaches the Secure Hash Algorithm (SHA-1) and its benefits [pages 442-445].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rogaway so that the hashing function was the Secure Hash Algorithm (SHA-1)

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rogaway by the teaching of Schneier because there are no

known cryptographic attacks against SHA and it is more resistant to brute-force attacks [page 445].

8. Claims 15 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, III U.S. Patent No. 5,204,902 as applied to claims 10 and 16 above, and further in view of Applied Cryptography (hereinafter Schneier).

As to claims 15 and 20, Reeds discloses using hash functions, as discussed above.

Reeds does not teach that the hash function is the Secure Hash Algorithm (SHA-1).

Schneier teaches the Secure Hash Algorithm (SHA-1) and its benefits [pages 442-445].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reeds so that the hashing function was the Secure Hash Algorithm (SHA-1)

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reeds by the teaching of Schneier because there are no known cryptographic attacks against SHA and it is more resistant to brute-force attacks [page 445].

Conclusion

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
August 5, 2004

E. Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER
8/11 2136